REMARKS

In the Office Action[1], the Examiner rejected claims 1-11 and 15-17 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,768,382 to Schneier et al. ("*Schneier*"), in view of U.S. Patent No. 5,671,412 to Christiano ("*Christiano*"), and further in view of U.S. Patent No. 5,629,980 to Stefik et al. ("*Stefik*"); rejected claims 18-22 under 35 U.S.C. § 103(a) as unpatentable over *Schneier*, in view of *Christiano*, in view of *Stefik*, and further in view of U.S. Patent No. 5,590,288 to Castor et al. ("*Castor*"); and rejected claim 57 under 35 U.S.C. § 103(a) as unpatentable over *Christiano* in view of *Stefik*.

Applicants have amended claims 1-3, 5, 7-11, 15-22, and 57 and canceled claims 4 and 6. Upon entry of this amendment, claims 1-3, 5, 7-11, 15-22, and 57 will remain pending.

Applicants respectfully traverse the rejection of claims 1-3, 5, 7-11, 15-22, and 57 under 35 U.S.C. § 103(a).

Claim 1 recites a data processing apparatus including, for example:

> . . .
> a hash-value generating circuit that generates hash values of the content data, the content key data, and the usage control policy data;
> a public key encryption circuit that creates signature data using the hash values and verifies the integrity of the signature data
> . . .

(emphasis added). *Schneier* does not teach or suggest the combination of the claimed "hash-value generating circuit" and "public key encryption circuit." The

[1] The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicants decline to automatically subscribe to any statement or characterization in the Office Action.

Examiner states that col. 17, lines 46-50 of *Schneier* discloses the claimed "hash-value generating circuit" (Office Action at page 8). Applicants respectfully disagree.

This passage of *Schneier* discloses a digital signature algorithm that is used to sign a message. The message may be "a hash value of the software generated with a one-way hash function, a compressed value of the software code produced by a compression algorithm, and the like." According to this passage, a digital signature algorithm may sign a message that may be a hash value of the software. Applicants find no teaching in this passage or any other passage of *Schneier* of that claimed "hash-value generating circuit" that generates 1) "hash values of the content data," 2) "the content key data," and 3) "the usage control policy data," as recited in claim 1.

In addition, claim 1 also recites "a public key encryption circuit" that 1) "creates signature data using the hash values" and 2) "verifies the integrity of the signature data." The Examiner cites col. 10, lines 27-56 of *Schneier* to disclose the claimed "public key encryption circuit."

Even assuming that this passage of *Schneier* discloses public key encryption, which Applicants do not concede, the encryption with a public key taught by *Schneier* does not create "signature data" using "hash values" and "verify the integrity of the signature data." Therefore, *Schneier* does not teach or suggest the claimed combination of elements including, for example, "a hash-value generating circuit that generates hash values of the content data, the content key data, and the usage control policy data [and] a public key encryption circuit that creates signature data using the hash values and verifies the integrity of the signature data," as recited in claim 1.

Christiano does not cure the deficiencies of *Schneier*. *Christiano* discloses a license server that "provides package and program licenses and allows several license modifiers to be stored in license records . . ." (col. 3, lines 14-16). *Christiano* does not teach or suggest the claimed combination of elements including, for example, "a hash-value generating circuit that generates hash values of the content data, the content key data, and the usage control policy data [and] a public key encryption circuit that creates signature data using the hash values and verifies the integrity of the signature data," as recited in claim 1.

Stefik does not cure the deficiencies of *Schneier* and *Christiano*. The Examiner states that col. 42, lines 49-55 of *Stefik* discloses the claimed "hash-value generating circuit" (Office Action at page 8). Applicants respectfully disagree.

This passage of *Stefik* discloses a requester that decrypts the software and "computes a check code on it using a 1-way hash function." While *Stefik* mentions the word "hash," *Stefik* does not teach or suggest a "hash-value generating circuit" that generates 1) "hash values of the content data," 2) "the content key data," and 3) "the usage control policy data," as recited in claim 1.

In addition, claim 1 also recites "a public key encryption circuit" that 1) "creates signature data using the hash values" and 2) "verifies the integrity of the signature data." The Examiner cites col. 26, line 65 - col. 27, line 9 of *Stefik* to disclose the claimed "public key encryption circuit."

This passage of *Stefik* discloses message transmission where "all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique." While *Stefik* mentions the words "public key

encryption," the public key encryption taught by *Stefik* does not create "signature data" using "hash values" and "verify the integrity of the signature data." Therefore, *Stefik* also does not teach or suggest the claimed combination of elements including, for example, "a hash-value generating circuit that generates hash values of the content data, the content key data, and the usage control policy data [and] a public key encryption circuit that creates signature data using the hash values and verifies the integrity of the signature data," as recited in claim 1.

Accordingly, *Schneier*, *Christiano*, and *Stefik* fail to establish a *prima facie* case of obviousness with respect to claim 1. Claim 1 is therefore allowable for at least the reasons presented above. Claims 2-11 and 15-16 depend from claim 1 and are thus also allowable for at least the same reasons as claim 1.

Independent claims 17 and 57, though of different scope from claim 1, are allowable for at least the same reasons as claim 1.

Although the Examiner cites *Castor* in the rejection of dependent claims 18-22, Applicants respectfully assert that *Castor* fails to cure the deficiencies of *Schneier*, *Christiano*, and *Stefik* discussed above. Therefore, claims 18-22 are also allowable at least due to their dependence from claim 17.

Applicants respectfully request that this Amendment under 37 C.F.R. § 1.116 be entered by the Examiner, placing claims 1-3, 5, 7-11, 15-22, and 57 in condition for allowance. This Amendment should allow for immediate action by the Examiner.

Furthermore, Applicants respectfully point out that the final action by the Examiner presented some new arguments against Applicants' invention. It is

respectfully submitted that the entering of the Amendment would allow the Applicants to reply to the final rejections and place the application in condition for allowance.

Finally, Applicants submit that the entry of the amendment would place the application in better form for appeal, should the Examiner dispute the patentability of the pending claims.

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration of the application and withdrawal of the rejections. Pending claims 1-3, 5, 7-11, 15-22, and 57 are in condition for allowance, and Applicants request a favorable action.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 17, 2008

By: /David W. Hill/
David W. Hill
Reg. No. 28,220